



Konfiguration der Windows Firewall von Microsoft® Windows® XP Service Pack 2 über eine INF-Datei

Microsoft Corporation

Veröffentlicht: März 2004

Zusammenfassung

Das Microsoft Windows XP Service Pack 2 (SP2) bringt umfangreiche Erweiterungen der Windows Firewall-Komponente mit sich. Die neue Windows Firewall (früher bekannt unter dem Namen Internetverbindungsfirewall) blockiert nicht erwünschten Netzwerkverkehr und sorgt damit für einen wirksamen Schutz des Computers vor schädlichen Programmen oder böswilligen Benutzern. Im Gegensatz zu früher ist unter Windows XP SP2 die Windows Firewall standardmäßig aktiviert. Netzwerkadministratoren können diese Standardaktivierung und die Standardeinstellungen jedoch vor oder nach der Installation über eine INF-Datei (Netfw.inf) verändern. Lesen Sie in diesem Artikel, wie Sie die Datei Netfw.inf für die Konfiguration der Windows Firewall verwenden.

Dies ist ein vorläufiges Dokument. Es könnte vor der endgültigen kommerziellen Veröffentlichung der hier beschriebenen Software grundlegende Änderungen erfahren.

Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der Microsoft Corporation zum Zeitpunkt der Veröffentlichung dar. Da Microsoft auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens Microsoft dar, und Microsoft kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren.

Dieses Dokument dient nur zu Informationszwecken. MICROSOFT SCHLIESST FÜR DIESES DOKUMENT JEDE GEWÄHRLEISTUNG AUS, SEI SIE AUSDRÜCKLICH ODER KONKLUDENT.

Die Benutzer/innen sind verpflichtet, sich an alle anwendbaren Urheberrechtsgesetze zu halten. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der Microsoft Corporation kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.) dies geschieht.

Es ist möglich, dass Microsoft Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von Microsoft eingeräumt.

© 2003 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, Active Directory und Windows sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere in diesem Dokument aufgeführte Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

Inhaltsverzeichnis

Übersicht.....	1
Szenarien, in denen die Standardkonfiguration der Windows Firewall geändert werden könnte.....	1
Aktivierte Firewall eines Drittanbieters.....	1
Vorinstallierte Programme.....	1
Standardmäßig geöffnete Ports.....	1
Speicherort der Windows Firewall-INF-Datei.....	1
Verfahren, um die standardmäßige Konfiguration der Windows Firewall zu ändern.....	2
Verfahren 1: Vor der Installation.....	2
Verfahren 2: Nach der Installation.....	2
Die standardmäßige INF-Datei.....	2
Mögliche Konfigurationsoptionen in der INF-Datei.....	3
Den Standard-Betriebsmodus der Windows Firewall ändern.....	4
Benachrichtigungen der Windows Firewall deaktivieren.....	5
Unicast-Antworten auf Multicast- und Broadcast-Pakete blockieren.....	5
Remoteadministration aktivieren.....	5
ICMP-Pakete zulassen.....	6
Statische Ports zur standardmäßigen Liste der Ausnahmen hinzufügen.....	7
Programme zur standardmäßigen Liste der Ausnahmen hinzufügen.....	8
Den Bereich für einen Eintrag in der INF-Datei definieren.....	9
Zusammenfassung.....	10
Zusätzliche Informationen.....	10

Übersicht

Die Windows Firewall von Windows XP Service Pack 2 (SP2) verwirft den gesamten Netzwerkverkehr, der nicht als Antwort auf eine Anfrage vom Computer gesendet wird (erwünschter Netzwerkverkehr) oder nicht als zugelassen definiert wurde (ausgenommener Netzwerkverkehr).

Die Windows Firewall wird während der Installation von Windows XP bzw. während der Installation von SP2 automatisch aktiviert. Netzwerkadministratoren müssen daher in der Lage sein, ihre Konfiguration vor und nach der Installation automatisch zu ändern. Eine typische Konfigurationsänderung wäre zum Beispiel das Hinzufügen von Programmen zur Ausnahmeliste oder auch das Deaktivieren der Windows Firewall (zum Beispiel, weil bereits eine Firewall eines Drittanbieters verwendet wird).

Die Windows Firewall kann über eine INF-Datei mit dem Namen Netfw.inf vorkonfiguriert werden – diese enthält die Standardkonfiguration. Während der Installation von Windows XP mit SP2 oder während des Updates auf SP2 wird die Konfiguration der Windows Firewall aus der INF-Datei importiert.

Szenarien, in denen die Standardkonfiguration der Windows Firewall geändert werden könnte

Die folgenden drei Szenarien erfordern zum Beispiel eine Änderung der Standardkonfiguration der Windows Firewall.

Aktivierte Firewall eines Drittanbieters

Ein OEM (Original Equipment Manufacturer) könnte zum Beispiel eine Firewall eines Drittanbieters installieren. Wenn diese standardmäßig aktiviert ist, dann sollte die Windows Firewall deaktiviert sein. Dies ist über die INF-Datei möglich.

Vorinstallierte Programme

Ein OEM oder ein Unternehmen könnte sich dazu entscheiden, standardmäßig eine bestimmte Gruppe von Programmen zu installieren. Einige dieser Programme sind möglicherweise von unverlangtem Netzwerkverkehr abhängig. Daher kann die Windows Firewall vorab so konfiguriert werden, dass der entsprechende Netzwerkverkehr zugelassen wird. Sie können hierzu Einträge für die entsprechenden Programme in die INF-Datei aufnehmen.

Standardmäßig geöffnete Ports

In einem Unternehmen sind unter Umständen unterschiedliche Netzwerkdienste im Einsatz – beispielsweise die in Windows XP integrierte Remoteadministration. Deshalb muss sichergestellt sein, dass der Netzwerkverkehr dieser Dienste nicht von der Windows Firewall blockiert wird. Die notwendigen TCP- und UDP-Ports können über die INF-Datei geöffnet werden.

Speicherort der Windows Firewall-INF-Datei

Sie finden die INF-Datei für die Windows Firewall auf der Windows XP-CD unter **CD_Laufwerk:\I386\Netfw.in_**

Anmerkung: Der Dateiname auf der Windows XP-CD lautet **Netfw.in_** (nicht Netfw.inf) – dies hängt mit der Dateisignatur zusammen.

Nach der Installation von Windows XP SP2 befindet sich die INF-Datei unter **%windir%\Inf\Netfw.inf**

Verfahren, um die standardmäßige Konfiguration der Windows Firewall zu ändern

Verfahren 1: Vor der Installation

1. Kopieren Sie die INF-Datei (**Netfw.in_**) von der Windows XP SP2-CD.
2. Nehmen Sie die erforderlichen Änderungen an der INF-Datei vor. Weitere Informationen hierzu finden Sie weiter unten im Abschnitt *Mögliche Konfigurationsoptionen in der INF-Datei*.
3. Speichern Sie die geänderte INF-Datei als **Netfw.in_**.
4. Signieren Sie die geänderte Datei **Netfw.in_**.
5. Ersetzen Sie die standardmäßige Datei **Netfw.in_** mit der geänderten Datei.
6. Installieren Sie Windows XP SP2.

Verfahren 2: Nach der Installation

1. Kopieren Sie die INF-Datei (**Netfw.inf**) von einer Windows XP SP2-Installation.
2. Nehmen Sie die erforderlichen Änderungen an der INF-Datei vor. Weitere Informationen hierzu finden Sie weiter unten im Abschnitt *Mögliche Konfigurationsoptionen in der INF-Datei*.
3. Speichern Sie die geänderte INF-Datei als **Netfw.inf**.
4. Ersetzen Sie die standardmäßige Datei **Netfw.inf** der Windows XP SP2-Installation mit der geänderten Datei.
5. Führen Sie für die Windows XP SP2-Installation, deren INF-Datei Sie geändert haben, den Befehl **netsh firewall reset** aus – entweder manuell oder über ein Script.

Die standardmäßige INF-Datei

In der Standardversion sieht die Datei Netfw.inf folgendermaßen aus:

```
[version]
```

```
Signature = "$Windows NT$"
```

```
DriverVer = 07/01/2001,5.1.2600.2096
```

```
[DefaultInstall]
```

```
AddReg=ICF.AddReg.DomainProfile
```

```
AddReg=ICF.AddReg.StandardProfile
```

```
[ICF.AddReg.DomainProfile]
```

```
HKLM, "SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List", "%windir%\system32\sessmgr.exe", 0x00000000, %REMOTE_ASSISTANCE%
```

```
[ICF.AddReg.StandardProfile]
```

```
HKLM, "SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List", "%windir%\system32\sessmgr.exe", 0x00000000, %REMOTE_ASSISTANCE%
```

```
[Strings]
```

```
REMOTE_ASSISTANCE = "%windir%\system32\sessmgr.exe:*:enabled:Remote Assistance"
```

Die ersten beiden Abschnitte enthalten die Versions- und Konfigurationsinformationen und müssen nicht geändert werden. Die änderbaren Abschnitte sind:

- **ICF.AddReg.DomainProfile**
Die Windows Firewall nutzt zwei unterschiedliche Konfigurationssätze – diese werden Profile genannt. Ein Profil wird verwendet, wenn der Computer mit der Domäne verbunden ist, der er angehört. Das andere Profil wird in allen anderen Fällen verwendet. Dieser Abschnitt enthält die Einstellungen für das Domänenprofil.
- **ICF.AddReg.StandardProfile**
Dieser Abschnitt enthält die Einstellungen für das Standardprofil – es wird verwendet, wenn der Computer nicht mit der eigenen Domäne verbunden ist. Wenn der Computer kein Domänenmitglied ist, wird ausschließlich das Standardprofil verwendet.
- **Strings**
Dieser Abschnitt definiert Datenstrings für die Einträge in den Abschnitten ICF.AddReg.DomainProfile und ICF.AddReg.StandardProfile.

Mögliche Konfigurationsoptionen in der INF-Datei

Über die INF-Datei kann ein Großteil der Windows Firewall-Standardeinstellungen angepasst werden. Hierzu gehören unter anderem:

- Betriebsmodus
- Deaktivieren von Benachrichtigungen
- Blockieren von Unicast-Antworten auf Multicast- und Broadcast-Pakete
- Aktivieren der Remoteadministration
- Zulassen von ICMP-Paketen
- Öffnen von Ports
- Zulassen von Programmen

Diese Einstellungen werden in den folgenden Abschnitt genauer beschrieben.

Anmerkungen: Die Einstellungen der INF-Datei werden auf alle Netzwerkschnittstellen des Computers angewandt. Es ist nicht möglich, für eine bestimmte Schnittstelle Ports zu öffnen oder ICMP-Pakete zu aktivieren. Protokolleinstellungen können über die INF-Datei nicht konfiguriert werden.

Den Standard-Betriebsmodus der Windows Firewall ändern

Die Windows Firewall unterstützt drei Betriebsmodi:

- **Aktiv**
Dies ist der Standardmodus der Windows Firewall. Der nicht angeforderte Netzwerkverkehr wird blockiert – die in der Ausnahmeliste definierten Einträge sind hiervon jedoch nicht betroffen. Da es sich um den Standardmodus handelt, muss zu seiner Konfiguration keine Änderung in der INF-Datei vorgenommen werden.
 - Die Einträge für das Domänenprofil befinden sich im Abschnitt **ICF.AddReg.DomainProfile** und lauten:
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile","DoNotAllowExceptions",0x00010001,0
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile","EnableFirewall",0x00010001,1
 - Die Einträge für das Standardprofil befinden sich im Abschnitt **ICF.AddReg.StandardProfile** und lauten:
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile","DoNotAllowExceptions",0x00010001,0
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile","EnableFirewall",0x00010001,0x00000001
 - **Aktiv (ohne Ausnahmen)**
In diesem Modus blockiert die Windows Firewall den gesamten nicht angeforderten Netzwerkverkehr – auch die Einträge in der Ausnahmeliste sind betroffen.
 - Um diesen Betriebsmodus für das Domänenprofil zu aktivieren, fügen Sie dem Abschnitt **ICF.AddReg.DomainProfile** die folgenden Einträge hinzu:
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile","DoNotAllowExceptions",0x00010001,1
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile","EnableFirewall",0x00010001,1
 - Um diesen Betriebsmodus für das Standardprofil zu aktivieren, fügen Sie dem Abschnitt **ICF.AddReg.StandardProfile** die folgenden Einträge hinzu:
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile","DoNotAllowExceptions",0x00010001,1
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile","EnableFirewall",0x00010001,1
 - **Inaktiv**
In diesem Modus filtert die Windows Firewall keinen Netzwerkverkehr.
 - Um diesen Betriebsmodus für das Domänenprofil zu aktivieren, fügen Sie dem Abschnitt **ICF.AddReg.DomainProfile** die folgenden Einträge hinzu:
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile","DoNotAllowExceptions",0x00010001,0
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile","EnableFirewall",0x00010001,0
-

- Um diesen Betriebsmodus für das Standardprofil zu aktivieren, fügen Sie dem Abschnitt **ICF.AddReg.StandardProfile** die folgenden Einträge hinzu:
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile","DoNotAllowExceptions",0x00010001,0
 - HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile","EnableFirewall",0x00010001,0

Benachrichtigungen der Windows Firewall deaktivieren

Wenn ein Programm, das noch nicht in der Ausnahmenliste der Windows Firewall enthalten ist, sich selbst über die Windows Firewall-APIs zur Ausnahmenliste hinzufügen will, dann wird der Benutzer benachrichtigt. Diese Benachrichtigungen können für beide Profile unterdrückt werden.

- Um die Benachrichtigungen für das Domänenprofil zu deaktivieren, fügen Sie dem Abschnitt **ICF.AddReg.DomainProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile","DisableNotifications",0x00010001,1
- Um die Benachrichtigungen für das Standardprofil zu deaktivieren, fügen Sie dem Abschnitt **ICF.AddReg.StandardProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile","DisableNotifications",0x00010001,1

Unicast-Antworten auf Multicast- und Broadcast-Pakete blockieren

Standardmäßig lässt die Windows Firewall nach einem Multicast- oder Broadcast-Paket an dem entsprechenden Port eingehende Unicast-Pakete für drei Sekunden lang zu. Dieses Verhalten kann über die INF-Datei deaktiviert werden.

- Um Unicast-Antworten auf Multicast- und Broadcast-Pakete für das Domänenprofil zu deaktivieren, fügen Sie dem Abschnitt **ICF.AddReg.DomainProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile","DisableUnicastResponsesToMulticastBroadcast",0x00010001,1
- Um Unicast-Antworten auf Multicast- und Broadcast-Pakete für das Standardprofil zu deaktivieren, fügen Sie dem Abschnitt **ICF.AddReg.StandardProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile","DisableUnicastResponsesToMulticastBroadcast",0x00010001,1

Remoteadministration aktivieren

Die zur Remoteadministration erforderliche RPC-Kommunikation (Remote Procedure Call) und DCOM-Kommunikation (Distributed Component Object Model) kann zugelassen werden. Wenn diese Option aktiviert wird, dann werden die TCP-Ports 135 und 445 für eingehenden Netzwerkverkehr geöffnet. Auch die Kommunikation über Named-Pipes wird gestattet. Windows-Dienste, die RPC verwenden, können weitere Ports dynamisch öffnen.

- Um die Remoteadministration für das Domänenprofil zu aktivieren, fügen Sie dem Abschnitt **ICF.AddReg.DomainProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Domain Profile\RemoteAdminSettings","Enabled",0x00010001,1

- Um die Remoteadministration für das Standardprofil zu aktivieren, fügen Sie dem Abschnitt **ICF.AddReg.StandardProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\RemoteAdminSettings","Enabled",0x00010001,1

Wenn Sie die Remoteadministration aktivieren, können Sie die IP-Adressen, von denen unverlangter Netzwerkverkehr zugelassen wird, auf einen bestimmten Bereich einschränken.

- Um einen IP-Bereich für das Domänenprofil zu definieren, fügen Sie dem Abschnitt **ICF.AddReg.DomainProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Domain Profile\RemoteAdminSettings","RemoteAddresses",0x00000000,**Bereich**

- Um einen IP-Bereich für das Standardprofil zu definieren, fügen Sie dem Abschnitt **ICF.AddReg.StandardProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\RemoteAdminSettings","RemoteAddresses",0x00000000,**Bereich**

Die möglichen Werte für den Parameter *Bereich* finden Sie im weiter unten im Abschnitt *Den Bereich für einen Eintrag in der INF-Datei definieren* dieses Artikels.

ICMP-Pakete zulassen

In der Standardkonfiguration blockiert die Windows Firewall alle ICMP-Pakete. Dieses Verhalten kann jedoch für die einzelnen ICMP-Nachrichtentypen geändert werden.

- Um ICMP-Nachrichtentypen für das Domänenprofil zuzulassen, fügen Sie dem Abschnitt **ICF.AddReg.DomainProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Domain Profile\IcmpSettings","**ICMP-Nachrichtentyp**",0x00010001,1

- Um ICMP-Nachrichtentypen für das Standardprofil zuzulassen, fügen Sie dem Abschnitt **ICF.AddReg.StandardProfile** den folgenden Eintrag hinzu:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\IcmpSettings","**ICMP-Nachrichtentyp**",0x00010001,1

Die gültigen Werte für den Parameter *ICMP-Nachrichtentyp* finden Sie in Tabelle 1.

Tabelle 1: ICMP-Nachrichtentypen

ICMP-Nachrichtentyp	Nummer	Beschreibung
AllowOutboundPacketTooBig	2	Wenn ein IPv6-Paket (Internet Protocol Version 6) zu groß ist um weitergeleitet zu werden, dann werden die Daten verworfen. Der Absender wird in so einem Fall mit diesem ICMP-Paket benachrichtigt.
AllowOutboundDestinationUnreachable	3	Wenn eine Übertragung wegen eines Fehlers fehlgeschlagen ist, dann wird der Absender mit diesem ICMP-Paket benachrichtigt.
AllowOutboundSourceQuench	4	Wenn der Computer die Menge der gesendeten Daten nicht

		verarbeiten kann, werden die Daten verworfen. Der Absender wird mit diesem Paket darüber benachrichtigt, dass er die Daten langsamer senden soll.
AllowRedirect	5	Die Daten werden neu geroutet.
AllowInboundEchoRequest	8	Die Pakete werden an den Absender zurückgeschickt. Diese Konfiguration wird normalerweise zur Fehlersuche verwendet (zum Beispiel bei einem Ping).
AllowInboundRouterRequest	10	Ein Computer antwortet auf ein Router-Discovery-Paket.
AllowOutboundTimeExceeded	11	Wenn ein Computer ein Paket verwirft, weil dessen Abschnittszähler zu hoch ist, oder weil er die Fragmente des Pakets nicht wieder zusammensetzen kann, wird der Absender mit dieser ICMP-Meldung benachrichtigt.
AllowOutboundParameterProblem	12	Wenn ein Computer Daten wegen eines fehlerhaften Headers verwirft, dann wird der Absender mit dieser ICMP-Meldung benachrichtigt.
AllowInboundTimestampRequest	13	Eingehende Pakete können mit dieser Bestätigungsnachricht beantwortet werden. Sie zeigt dem Absender, wann die Daten empfangen wurden.
AllowInboundMaskRequest	17	Computer warten auf Anfragen für Subnetzmasken und antworten auch auf diese Anfragen.

Statische Ports zur standardmäßigen Liste der Ausnahmen hinzufügen

Unter Windows XP SP2 verwaltet die Windows Firewall für jedes der beiden Profile eine Ausnahmeliste. Die Ports aus dieser Liste sind im normalen Betrieb statisch geöffnet. Im Allgemeinen wird eher empfohlen, dass Sie Programme zur Ausnahmeliste hinzufügen. Die Windows Firewall kann so Ports dynamisch öffnen und schließen, und die Zahl der offenen Ports kann so möglichst klein gehalten werden. Es gibt allerdings einige Szenarien, in denen statisch geöffnete Ports notwendig sind – zum Beispiel bei der Verwendung bestimmter Windows-Dienste.

- Um einen statischen Port zur Ausnahmeliste des Domänenprofils hinzuzufügen, tragen Sie den folgenden Wert im Abschnitt **ICF.AddReg.DomainProfile** ein:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\GloballyOpenPorts\List","Portnummer:Protokoll",0x00000000,%StringFürDenPorteintrag%
```

- Um einen statischen Port zur Ausnahmeliste des Standardprofils hinzuzufügen, tragen Sie den folgenden Wert im Abschnitt **ICF.AddReg.StandardProfile** ein:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List","Portnummer:Protokoll",0x00000000,%StringFürDenPorteintrag%
```

Beide Einträge beziehen sich jeweils auf einen String. Dieser String muss sich im Abschnitt **[Strings]** befinden, und er verwendet das folgende Format:

```
StringFürPorteintrag = "Portnummer:Protokoll:Bereich:Modus:AngezeigterPortname"
```

Hierbei haben die einzelnen Teile des Strings die folgenden Bedeutungen:

- StringFürPorteintrag*
Ein Verweis auf einen Eintrag im Abschnitt **ICF.AddReg.DomainProfile** oder **ICF.AddReg.StandardProfile**, zu dem dieser String gehört.

- *Portnummer*
Die Portnummer zwischen **1** und **65535**.
- *Protokoll*
Das Protokoll für diesen Port – entweder **TCP** oder **UDP**.
- *Bereich*
Die möglichen Werte für diesen Parameter finden Sie weiter unten in diesem Artikel im Abschnitt *Den Bereich für einen Eintrag in der INF-Datei definieren*.
- *Modus*
Ein Eintrag in der Ausnahmenliste kann entweder aktiviert (der Port wird statisch geöffnet) oder deaktiviert (der Port wird nicht statisch geöffnet) sein. Daher sind die beiden möglichen Werte für diesen Parameter **enabled** und **disabled**.
- *AngezeigterPortname*
So wird der Eintrag in der Konfiguration der Windows Firewall in der Systemsteuerung angezeigt. Er sollte aussagekräftig sein und klar definieren, warum dieser Port statisch geöffnet wurde – zum Beispiel "Webserver (TCP 80)" oder "Telnet-Server (TCP 23)".

Um einen Port in beiden Profilen statisch zu öffnen, sind also drei Einträge in der INF-Datei notwendig. Im folgenden Beispiel wird der UDP-Port 500 statisch geöffnet. Dieser wird von IKE (Internet Key Exchange Protocol) verwendet. Als Bereich werden alle IP-Adressen festgelegt.

- Der folgende Eintrag wird zum Abschnitt **ICF.AddReg.DomainProfile** hinzugefügt:
`HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\GloballyOpenPorts\List","500:UDP",0x00000000,%IKE%`
- Dieser Eintrag wird zum Abschnitt **ICF.AddReg.StandardProfile** hinzugefügt:
`HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List","500:UDP",0x00000000,%IKE%`
- Und schließlich wird dieser Eintrag zum Abschnitt **Strings** hinzugefügt:
`IKE = "500:UDP:*.enabled:IKE (UDP 500)"`

Programme zur standardmäßigen Liste der Ausnahmen hinzufügen

Es ist zusätzlich möglich, Programme zur Ausnahmeliste hinzuzufügen. Für diese Programme werden dann die entsprechenden Ports dynamisch von der Windows Firewall geöffnet.

- Um ein Programm zur Ausnahmeliste des Domänenprofils hinzuzufügen, tragen Sie den folgenden Wert im Abschnitt **ICF.AddReg.DomainProfile** ein:
`HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List","PfadZurAusführbarenDatei",0x00000000,%StringFürProgrammeintrag%`
- Um ein Programm zur Ausnahmeliste des Standardprofils hinzuzufügen, tragen Sie den folgenden Wert im Abschnitt **ICF.AddReg.StandardProfile** ein:
`HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List","PfadZurAusführbarenDatei",0x00000000,%StringFürProgrammeintrag%`

Beide Einträge beziehen sich jeweils auf einen String. Dieser String muss sich im Abschnitt **[Strings]** befinden, und er verwendet das folgende Format:

StringFürProgrammeintrag =
"PfadZurAusführbarenDatei:Bereich:Modus:AngezeigterProgrammname"

Hierbei haben die einzelnen Teile des Strings die folgenden Bedeutungen:

- *StringFürProgrammeintrag*
Ein Verweis auf einen Eintrag im Abschnitt **ICF.AddReg.DomainProfile** oder **ICF.AddReg.StandardProfile**, zu dem dieser String gehört.
- *PfadZurAusführbarenDatei*
Ein voll qualifizierter Pfad zur ausführbaren Datei des Programms (kann Umgebungsvariablen wie zum Beispiel %Path% enthalten).
- *Bereich*
Die möglichen Werte für diesen Parameter finden Sie weiter unten in diesem Artikel im Abschnitt *Den Bereich für einen Eintrag in der INF-Datei definieren*.
- *Modus*
Ein Eintrag in der Ausnahmenliste kann entweder aktiviert (Ports werden für das Programm dynamisch geöffnet) oder deaktiviert (Ports werden für das Programm nicht dynamisch geöffnet) sein. Daher sind die beiden möglichen Werte für diesen Parameter **enabled** und **disabled**.
- *AngezeigterProgrammname*
So wird der Eintrag in der Konfiguration der Windows Firewall in der Systemsteuerung angezeigt. Er sollte aussagekräftig sein und klar definieren, warum dieser Port statisch geöffnet wurde – zum Beispiel "MSN Messenger v6.1" oder "AOL Instant Messenger v5.5".

Um ein Programm zu beiden Profilen hinzuzufügen, sind also drei Einträge möglich. Die folgenden Beispieleinträge ermöglichen die Remoteunterstützung und legen als Bereich alle IP-Adressen fest.

- Dieser Eintrag wird zum Abschnitt **ICF.AddReg.DomainProfile** hinzugefügt:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List", "%windir%\system32\sessmgr.exe",0x00000000,%REMOTEUNTERSTUETZUNG%
- Dieser Eintrag wird zum Abschnitt **ICF.AddReg.StandardProfile** hinzugefügt:

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List", "%windir%\system32\sessmgr.exe",0x00000000,%REMOTEUNTERSTUETZUNG%
- Dieser Eintrag wird zum Abschnitt **Strings** hinzugefügt:

REMOTEUNTERSTUETZUNG =
"%windir%\system32\sessmgr.exe*:enabled:Remoteunterstützung"

Den Bereich für einen Eintrag in der INF-Datei definieren

Wenn Sie die Remoteunterstützung aktivieren, Ports öffnen oder Programme in die Ausnahmenliste eintragen, dann müssen Sie einen Bereich von IP-Adressen angeben, von denen unverlangt eingehender Netzwerkverkehr zugelassen wird. Hierbei gibt es drei Möglichkeiten:

- **Alle IP-Adressen**
Dies ist der Standardbereich für Ausnahmeeinträge. Er ermöglicht unverlangt eingehenden Netzwerkverkehr von allen IP-Adressen. Er wird mit einem Stern ("*") bezeichnet.
-

- **Nur lokales Subnetz**

Dieser Bereich beschränkt die IP-Adressen, von denen unverlangt eingehender Netzwerkverkehr angenommen wird, auf das Subnetz, mit dem die Netzwerkschnittstelle, über die der Netzwerkverkehr empfangen wurde, verbunden ist. Wenn sich das Subnetz einer Netzwerkschnittstelle ändert, dann ändert sich automatisch auch dieser Wert. Sie konfigurieren diesen Bereich, wenn Sie den Wert **LocalSubnet** angeben.

- **Benutzerdefiniert**

Bei einem benutzerdefinierten Bereich können Sie eine oder mehrere IP-Adressen und Subnetze angeben, von denen unverlangt eingehender Netzwerkverkehr angenommen wird. Sie können das lokale Subnetz mit in Ihren benutzerdefinierten Bereich einschließen. IPv6-Adressen sind jedoch nicht möglich. Um Subnetze anzugeben, können Sie entweder eine Subnetzmaske oder die CIDR-Notation verwenden. Die einzelnen Einträge werden jeweils durch ein Komma getrennt. Benutzerdefinierte Bereiche können zum Beispiel folgendermaßen aussehen:

- 192.168.0.5
- 192.168.0.0/255.255.255.0
- 192.168.0.5,LocalSubnet
- 157.54.0.1,172.16.0.0/12,10.0.0.0/255.0.0.0,LocalSubnet

Zusammenfassung

Um Windows XP SP2 mit angepassten Einstellungen für die Windows Firewall zu installieren oder deren Einstellungen nach der Installation von SP2 zu ändern, können Sie eine INF-Datei verwenden (Netfw.inf). Diese INF-Datei enthält drei Abschnitte: **ICF.AddReg.DomainProfile** zur Definition der Domänenprofil-Einstellungen der Windows Firewall, **ICF.AddReg.StandardProfile** zur Definition der Standardprofil-Einstellungen der Windows Firewall und **Strings** für die jeweiligen Datenstrings. Normalerweise wird die INF-Datei zur Deaktivierung der Windows Firewall – zum Beispiel, weil eine Firewall eines Drittanbieters im Einsatz ist – oder zum Hinzufügen von Programmen oder Ports zur Ausnahmeliste genutzt.

Zusätzliche Informationen

- [Windows XP Service Pack 2 - Einstellungen für die Windows Firewall bereitstellen](#)
 - [Windows XP Service Pack 2: Informationen für Entwickler](#) (englischsprachig)
 - [The Cable Guy - Februar 2004](#)
[Manuelle Konfiguration der Windows Firewall von Windows XP Service Pack 2](#)
 - Aktuelle Informationen zu Windows XP finden Sie auf der [Windows XP Website](#).
-